Lab 1.3.2 - Cracking Passwords with John the Ripper

Name: _____ Date: _____ Class: _____

Objectives: Apply a tool used for automated password cracking and identify the characteristics that make passwords vulnerable to these attack tools.

Background Information: Password attacks use software programs which automate the process of rapidly testing many potential passwords for a given account.

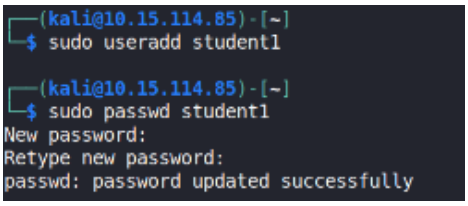
- **Brute Force Attack** = Attempts to guess a password by trying *all possible combinations of characters.*
- **Dictionary Attack** = Uses a database (AKA dictionary) of words that people are likely to use in their passwords including names of movies, teams, celebrities, foreign languages AND including spelling with numbers or special characters substituted for letters.
- **Hybrid Attack** = Dictionary + Brute Force
  The tool used in this lab, **John the Ripper**, will use the Hybrid Attack as it assumes most passwords can be found in cracking dictionaries and depends on fast, high volume guessing.

Instructions:

- Go to CYBER.ORG Range (https://apps.cyber.org)
- Click on the **Range tab**, then click on **Launch Kali**.
- Once the status changes to booted, click Open.
- Open a terminal by clicking the black square with the white border in the top left toolbar.

Part 1: Create users & passwords:

1. Change to the root folder:
   Type **`cd /`**
2. Create a user on the system:



   Type **`sudo useradd student1`**
3. Set a password for the user:
   Type **`sudo passwd student1`**
   At the prompt *"New password:"* type **`changeme`**
   At the prompt "*Retype new password:*" type **`changeme`**
4. Repeat steps to add the following users and passwords:

student2	7dwarfs
student3	porsche911
student4	1234567890
student5	trustno1

Part B: Locate the hashed Passwords:

In the Linux operating system the password hashes are stored in the /etc/shadow file. In earlier versions of Linux these hashes were stored in the /etc/passwd file but now that file only holds user information. Compare the two files:

1. At the terminal prompt type **`sudo cat /etc/shadow`**
2. Leave that terminal open and click on the terminal icon in the top toolbar to open a new terminal window.
3. Type **`sudo cat /etc/passwd`**
4. Put the two terminal windows side by side and scroll down to see the user names that you created. Observe the info stored for users in each file.
5. Close the new terminal window that has the /etc/passwd file info.

Part C: Use the John the Ripper tool to crack user passwords:

There are many password cracking apps but John the Ripper (JtR) has been around for a long time and is easy to install and execute.

1. Use JtR to perform a Dictionary password cracking attack which uses a wordlist to crack the password hashes. By default, John the Ripper detects the hash type and then tries to crack the password based on that type.
   Type **`sudo john /etc/shadow --wordlist=/usr/share/john/password.lst`**
   You should quickly see displayed the 5 usernames, their cracked passwords PLUS the root password.
   Important Note: If at any point you want to start over you must first clear the John buffer with this command: **`sudo rm /root/.john/john.pot`**

Q: How long did it take to crack all the passwords? [Time is listed after the passwords.] The format is Day:Hour:Minute:Seconds	
Q: Which password was cracked first? Give username and password	
Q: Which password was cracked last? Give username and password	

2. Examine the wordlist file used by John the Ripper by sending it to a text file in your home directory.
   Type:
   `sudo cat /usr/share/john/password.lst > /home/kali/JtRpass.txt`
   On the top toolbar click the Folder icon, select Open Folder.
   Scroll down and doubleclick on the JtRpass.txt file to open it.

   Q: Based on the info in the JtRpass.txt file, which password do you think would have been cracked first and which one last? Explain your answer.